Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132
Telephone: none
Email: none

Daniel David Rigmaiden
Pro Se, Defendant

**UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

| | |
|---|---|
| United States of America,<br>Plaintiff,<br>v.<br>Daniel David Rigmaiden, et al.,<br>Defendant. | No. CR08-814-PHX-DGC<br>STATEMENT OF THE ISSUES RE: INTERLOCUTORY APPEAL OF PORTION OF COURT'S ORDER (Dkt. #1009) DENYING Dkt. #847 AND Dkt. #927<br>[**F.R.A.P. 10(b)(3)(A)**] |

Defendant, Daniel David Rigmaiden, appearing *pro se*, hereby submits this statement of the issues pursuant to F.R.A.P. 10(b)(3)(A) in reference to his interlocutory appeal from the portion of the district court's May 8, 2013 order at Dkt. #1009 denying the defendant's motions at Dkt. #847 and #927. The issues the defendant raises on appeal are as follows:

1. Whether Appellant is suffering a deprivation of his Fourth Amendment rights through the government's indefinite retention and viewing of his personal, private, and privileged digital data (*i.e.*, data beyond the scope of two relevant warrants) contained on seized physical data storage devices and on government duplicates while *(a)* the government has already isolated and seized/copied all *in-scope* data under the warrants, *(b)* the warrants used to seize the physical data storage devices expressly require deletion of all *out-of-scope* data 90 days after the warrants' execution, and *(c)* the government has no use for the *out-of-scope* data.

2. Whether the district court erred in making the unsupported factual finding that

the prosecutor and case agents in Arizona contacted the USAO of the Northern District of California in order to obtain its interpretation of the "Computer Search Protocol For The Northern District Of California," as it is applies in the Northern District of California.

3. Whether the district court erred in making the unsupported factual finding that the Arizona case agents' and prosecutor's interpretation of the "Computer Search Protocol For The Northern District Of California" is precisely the same as how the protocol is interpreted in the Northern District of California.

4. Whether the district court erred in making the legal finding that the government acted in good-faith when it erroneously interpreted the "Computer Search Protocol For The Northern District Of California" to mean that the government is now permitted to indefinitely retain and view Appellant's *out-of-scope* data.

5. Whether the district court erred in making the legal finding that the government's purported good-faith interpretation of the "Computer Search Protocol For The Northern District Of California"—an interpretation the Arizona district court Judge found erroneous—justifies the government's indefinite violation of the protocol, indefinite retention and viewing of *out-of-scope* data beyond the specified 90-day period, and indefinite violation of Appellant's Fourth Amendment rights.

6. If the Northern District of California does, in fact, interpret the "Computer Search Protocol For The Northern District Of California" in the same manner as interpreted by the Arizona prosecutor and case agents (*i.e.*, permitting the government to indefinitely retain and view all *out-of-scope* data beyond the 90-day period specified in the protocol), whether the district court erred in making the legal finding that the Northern District of California interpretation is reasonable and justifies the now ongoing/indefinite retention and viewing of Appellant's *out-of-scope* data by the government in Arizona.

* * *

While the district court found that the "Computer Search Protocol For The Northern District Of California" requires that the government delete/destroy all *out-of-scope* data 90 days after execution of the warrants, it nevertheless held that the government can indefinitely

retain and view all *out-of-scope* data even while it has no use for the data:

> Paragraph 5 goes on to state that within a reasonable period, "not to exceed sixty calendar days after completing the authorized search of a device" – so this could be up to 90 days after the device was first seized – the government must destroy "copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process[.]"... **If read more literally**, the phrase could mean ***all* data not responsive to the warrant must be deleted within 90 days of seizure**... **The Court finds the literal reading to be more reasonable** – the specific phrase used in the protocol is "any data" – but the Court cannot conclude that the interpretation applied in the Northern District of California, where the protocol was created and applies, is wholly unreasonable. Nor can the Court conclude that government agents in Arizona should have known that the Northern District interpretation was so unreasonable as to be incorrect as a matter of law...
>
> *Court's May 8, 2013 Order* (Dkt. #1009, p. 40-41 (emphasis added)).
>
> To the extent the government's interpretation of the protocol was mistaken, the error was, at most, the product of negligence.
>
> *Id.* (Dkt. #1009, p. 49).
>
> The Court also concludes that the government has continued to search copies of the devices that contained relevant information... after the 30-day period specified in the protocol.
>
> *Id.* (Dkt. #1009, p. 38).
>
> This is not a case where the government engaged in a wide-ranging search for any possible kind of criminal activity. Material found by the government on Defendant's computer relates directly to the alleged tax-refund fraud; the government has not charged Defendant with new violations of law as a result of the search of his computer and storage devices....
>
> *Id.* (Dkt. #1009, p. 46).
>
> As noted above, the government represents that results of the search related only to the charged offenses and were not shared with agents or agencies outside the prosecution in this case....
>
> *Id.* (Dkt. #1009, p. 50).
>
> Defendant filed a Motion for Order Requiring Government to Comply with Data Deletion Requirements, requesting an order directing the government to delete or destroy data not originally seized by Agent Daun. [] Specifically, Defendant seeks an order requiring the government to locate and isolate all the physical data storage devices that were seized from his apartment and storage unit and sanitize (by overwriting the devices with random data) or physically destroy the devices, with the exception of the files and data listed in Agent Daun's 'Computer Forensic Report.' [] The government objects, contending that there is no authority for Defendant's demands. [] The Court agrees... The motion is denied.
>
> *Id.* (Dkt. #1009, p. 49-50).

First, the interpretation of the "Computer Search Protocol For The Northern District Of California," as it is interpreted in the Northern District of California, is precisely the same as Judge Campbell's "any data" interpretation in the present case:

> "The government... should not be retaining images of files or documents that, in large part, do not contain information within the scope of the warrant."
>
> United States v. Fu-Tain Lu, No. CR-09-00341 RMW, Doc. No. 112, p. 4 (**N.D.Cal.**, Sept. 16, 2010) (addressing images and government copies).
>
> "[E]ven if the law ultimately permits the forfeiture of a given device..., the law does not permit the retention of data on that device that has not been shown or even alleged to have been an 'instrumentality' of the alleged crimes."
>
> United States v. Collins, 2012 U.S. Dist. LEXIS 35980, Case No.: 11-CR-00471-DLJ (PSG), p. 12 (**N.D.Cal.**, Mar. 16, 2012) (addressing original devices).

Second, even if the Northern District of California does, in fact, interpret the "Computer Search Protocol For The Northern District Of California" in the same erroneous manner [despite *Fu-Tain Lu* and *Collins*] as interpreted by the Arizona prosecutor and case agents, this so-called "good faith" interpretation does not justify the continual violation of the protocol in light of Arizona district court Judge Campbell's interpretation being identical to the interpretation reached by other judges in the Northern District of California.

Third, regardless of the terms of the warrants, it is a clear Fourth Amendment violation for the government to indefinitely retain and view *out-of-scope* data on seized storage devices, forensic images, *etc.* that the case agents themselves admit "actually contain many more files than those that fall within the parameters of the Search Warrant and its attachments[]"[1] and the government indicates no valid use for the *out-of-scope* data.

Fourth, the portion of the district court's order at Dkt. #1009 denying the defendant's motions at Dkt. #847 and #927 is a final appealable order. *See* United States v. Griffin, 617 F.2d 1342 (9th Cir. 1980); Cohen v. Beneficial Industrial Load Corp., 337 U.S. 541 (1949). The order at Dkt. #1009 is a final determination of the issue in the district court, *i.e.*, the

---

1. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47, p. 31).

defendant is filing no motion for reconsideration of the specific portion of the order at issue. The challenged issue is also not a step toward final disposition of the case, *i.e.*, because the personal, private, and privileged *out-of-scope* data is not related to the merits of the case—or to any case for that matter—the ruling therefore has no effect on the outcome of the instant case or *any* case. Finally, the rights of Appellant would be irreparably lost if review is postponed until final judgment, *i.e.*, Appellant's Fourth Amendment rights are under a continual deprivation considering the government continues to retain and view his personal, private, and privileged *out-of-scope* data.

Therefore, the defendant is filing his interlocutory appeal to address this narrow issue that will survive the outcome of the case.

* * * * *

This statement of the issues was drafted by the *pro se* defendant, however, he authorizes his shadow counsel, Philip Seplow, to sign and file this statement on his behalf using the ECF system.

DANIEL DAVID RIGMAIDEN, Pro Se
Defendant:

s/ Daniel Rigmaiden

Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132

///

///

///

///

///

///

Respectfully Submitted: May 15, 2013

PHILP SEPLOW, Shadow Counsel, on behalf of DANIEL DAVID RIGMAIDEN, Pro Se Defendant:

s/ Philip Seplow
Philip Seplow
Shadow Counsel for Defendant.

CERTIFICATE OF SERVICE

I hereby certify that on: May 15, 2013 I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Taylor W. Fox, PC
Counsel for defendant Ransom Carter
2 North Central Ave., Suite 735
Phoenix, AZ 85004

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

By: s/ Daniel Colmerauer
(Authorized agent of Philip A. Seplow, Shadow Counsel for Defendant; See ECF Proc. I(D) and II(D)(3))